NATIONAL OCEANOGRAPHIC DATA CENTER

ISMD

INFORMATION SYSTEMS & MANAGEMENT DIVISION

ABOUT ISMD

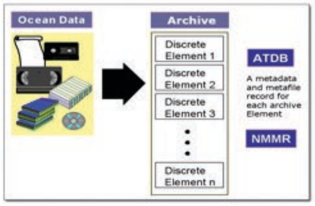
Mission

Provide information technology services which permit NODC to maintain global oceanographic data and information in a secure, sustainable, permanent archive, readily accessible to a diverse global user community.

Functions

- Manage & Operate NODC IT Infrastructure
- Manage & Preserve NODC's Digital Archive
- Manage IT Resource Planning & Reporting
- Ensure Integrity of NODC Digital Archive
- Ensure Access to NODC Digital Archive
- Interface with NOAA/NESDIS and other Federal Components

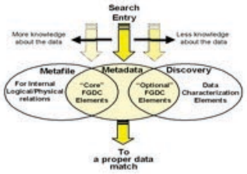
METADATA / ARCHIVE

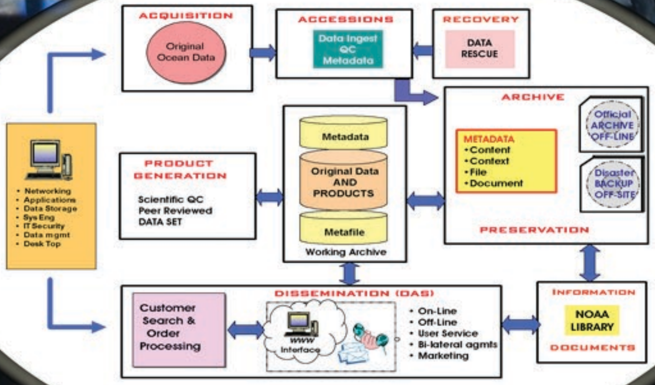


NODC Archive Principles:

- Preserve
- Protect
- Inventory
- Distribute
- Migrate
- Participate

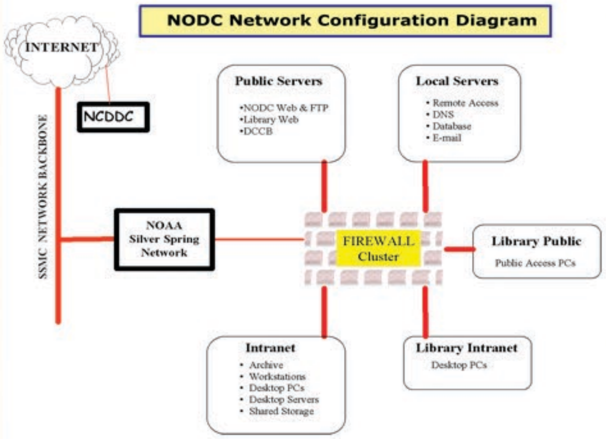
Metadata System


Search Entry
More knowledge about the data
Less knowledge about the data
Metafile
For Internal Logical/Physical relations
Metadata
"Core" FGDC Elements
"Optional" FGDC Elements
Discovery
Data Characterization Elements
To a proper data match



NETWORK

NODC Network Configuration Diagram



SECURITY / DESKTOP

Security

- Code Audits
- User Education
- Propose Security Policy
- Data Center Certification & Accreditation
- Develop Security Procedures
- Contingency & Disaster Recovery Planning
- COOP-Continuity of Operations
- Backup Systems & Restore Functionality
- Critical Software Upgrades
- Firewall Configuration & Maintenance
- Remote Access System
- Define / Maintain Standard Software Configurations

Desktop Support

- Educate and counsel users individually and in seminars
- Design, specify and requisition new systems and system enhancements
- Set and enforce policies regarding configuration and usage of computers
- Set up and maintain Windows and Macintosh desktop computer systems and networks
- Perform system analysis, make recommendations and provide management with milestone status reports
- Contribute to Office Support and IT Security policy advisory committees of NODC's parent agency, NESDIS

National Oceanographic Data Center

ISMD

Information Systems & Management Division

ISMD designs, procures, builds, and maintains NODC's computing infrastructure--desktops, servers, and networks--and provides many essential services to maintain the health of this infrastructure. ISMD regards infrastructure health and stability as critical to NODC's mission, so ISMD performs all of its tasks under a governing principle of protecting overall system health.

System security is an essential component of this principle--for this reason, ISMD focuses much of its energy on improving and maintaining security. All major software and hardware procurements are carefully considered in terms of their impact on security. Publicly exposed software components, such as data access portals, are audited by ISMD personnel to assure code correctness, and to eliminate vulnerabilities. ISMD personnel perform regular scans of all network-connected systems and devices to ensure all software is properly patched, and to identify unauthorized configuration changes. ISMD maintains an advanced network firewall that partitions NODC's networks into zones with distinct purposes--e.g. public access services, intranet services, remote access services--and enforces well-defined network policies to protect each zone independently, so that a compromise in one area will be effectively contained.

Another important aspect of system health is availability. ISMD employs many forms of hardware redundancy to minimize single points of failure and assure continued availability in the face of inevitable hardware problems. NODC's firewall is fully redundant and provides automatic failover. All servers utilize RAID technology to protect against disk failure. Core network interconnects use load-balanced, redundant paths for increased bandwidth and fault tolerance. Power to every server is provided on multiple UPS circuits on distinct power phases. ISMD maintains multiple generations of tape backups, and moves copies of these tapes to offsite storage to protect NODC's data in case the NODC site is destroyed. ISMD utilizes automated systems to periodically verify the availability of all critical network services and notify administrators immediately in the event of failures.

ISMD uses additional measures to protect NODC's data archive from corruption of any kind. All archive files are periodically verified against stored checksums so that any modification, however slight, will be detected in a timely manner. In such an event, ISMD will restore correct data from backup tape.

The ISMD team develops and maintains all documentation supporting NODC's FISMA certification and accreditation process. This documentation is crucial to retaining NODC's authority to operate as an accredited Federal government system.

ISMD personnel manage the entire life cycle of every computer system at NODC--procurement, installation of the hardware, operating system, and other software, continual software and hardware maintenance, and eventual media sanitizing and excessing of property--all with the objective of keeping NODC's infrastructure functioning smoothly. In addition, ISMD personnel provide technical support to assist NODC users in getting the most out of NODC's computing resources. The ISMD team takes pride in its mission to support NODC.